2000-09

Requirements analysis and infrastructure assessment methodologies for intranet development.

Sizemore, Scott R.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

REQUIREMENTS ANALYSIS AND INFRASTRUCTURE ASSESSMENT METHODOLOGIES FOR INTRANET DEVELOPMENT

by

Scott R. Sizemore

September 2000

Thesis Advisor:	Barry Frew
Thesis Associate Advisor:	William J. Haga

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2000	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE: Requirements Analysis and Infrastructure Assessment Methodologies for Intranet Development

5. FUNDING NUMBERS

6. AUTHOR(S) Sizemore, Scott R.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

This is a study of intranet planning methodologies with specific focus on two aspects of project planning, requirements analysis and infrastructure assessment. This thesis examines both qualitative and quantitative aspects of assessing and planning for intranets. Thoroughly completing these two areas is important in order to bring success to an intranet project. This thesis examines variables necessary in each area that require consideration during planning. Chapter II is a study of requirements analysis. A three-step methodology will guide planners through a logical process that assists in creating a well-organized plan. Chapter III is a study of infrastructure assessment. Items of infrastructure are defined and listed to assist planners to assess existing infrastructures. A five-step methodology will guide planners through a logical process of assessing enterprise infrastructure. Chapter IV is a case study of the U.S. Marine Corps Collaborative Planning Network, an enterprise-wide intranet project designed to augment the existing Marine Corps Enterprise Network. Methods and processes in this case study closely parallel methods of planning recommended in this thesis. Chapter V contains a summary and recommendations. This chapter also provides recommendations for areas of further study in intranet planning.

14. SUBJECT TERMS Computer Networks, Intranets			15. NUMBER OF PAGES 108
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

REQUIREMENTS ANALYSIS AND INFRASTRUCTURE ASSESSMENT METHODOLOGIES FOR INTRANET DEVELOPMENT

Scott R. Sizemore
Major U.S. Marine Corps
B.S., University of Utah, 1988

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

NAVAL POSTGRADUATE SCHOOL
September 2000

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This is a study of intranet planning methodologies with specific focus on two aspects of project planning, requirements analysis and infrastructure assessment. This thesis examines both qualitative and quantitative aspects of assessing and planning for intranets. Thoroughly completing these two areas is important in order to bring success to an intranet project. This thesis examines variables necessary in each area that require consideration during planning. Chapter II is a study of requirements analysis. A three-step methodology will guide planners through a logical process that assists in creating a well-organized plan. Chapter III is a study of infrastructure assessment. Items of infrastructure are defined and listed to assist planners to assess existing infrastructures. A five-step methodology will guide planners through a logical process of assessing enterprise infrastructure. Chapter IV is a case study of the U.S. Marine Corps Collaborative Planning Network, an enterprise-wide intranet project designed to augment the existing Marine Corps Enterprise Network. Methods and processes in this case study closely parallel methods of planning recommended in this thesis. Chapter V contains a summary and recommendations. This chapter also provides recommendations for areas of further study in intranet planning.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENT

The author would like to acknowledge those individuals who provided their support throughout the process of completing this thesis.

Professor Barry A. Frew, for providing guidance, advice, as well as challenging and provocative questions that required stretching of the mind. Also, for providing research space complete with everything necessary to work without the aggravation of interruptions.

Mrs. Marilyn Schneider, Professor Frew's Administrative Officer, for making me feel like part of the Center for Executive Education's family, and for her cheerfully making sure I had anything I needed.

Ms. Mary Redmond, Professor Frew's Administrative Assistant, for her warm welcomes, regularly stocked goodie jar, and always making a time slot available on Barry's hectic schedule, regardless of how many flag officers were on the same schedule.

Professor William J. Haga, for providing blunt suggestions to sharpen the wording of many paragraphs. In addition, for his sarcasm and sense of humor, it aids learning if you let it.

Mr. Steven Page, Mr. Ed Blackman, Mr. Jerry Redding, and Mr. Randy Watkins of the Marine Information Telecommunication Network Operations Center, who provided data and insight for the case study of the Collaborative Planning Network.

Mr. Craig Opel, LtCol USMC (Ret.), for suggesting that I attend NPS in the first place. Also for his keen insight, leadership by example, and ability to make the best of any situation.

Major David McMorries USMC, for his valuable friendship, quick wit, and sanity checks of many chapters.

Ms. Nancy Sharrock, of the Applications Development Group, for taking time to help with advanced formatting requirements.

Lastly but certainly not least, I dedicate this thesis and Master's Degree to my beautiful family, Christi, my precious wife of nearly 15 years, and three wonderful children, Colton, Hayley, and Emily Sizemore. With your lovingly faithful support, I have successfully completed this thesis and degree. Thanks for all the warm hugs that kept me going in times of need.

I. INTRODUCTION

> An intranet is a private computer network that uses Internet standards and protocols to enable members of an organization to communicate and collaborate more efficiently with one another, thereby increasing productivity. [Ref. 13]

As intranet technology continues to permeate organizations and claim to increase productivity, collaboration and make people more efficient, many organizations have rushed to their IT department and clamored to get on the intranet band wagon. Many organizations have successfully implemented intranets while some have failed. This thesis describes elements, procedures necessary to successfully and implement an intranet. The word implementation means more than installation of computers and networks. In this thesis, implementation is meant to describe the iterative process of analyzing requirements, planning, designing, testing, revising, installing and maintaining an intranet.

A. BACKGROUND

As the Department of Defense (DoD) and the Department of the Navy (DoN) continue searching for ways to leverage information technology to improve efficiency and effectiveness, intranet technology has surfaced as the answer to many communication and collaborative requirements. With technology becoming increasingly affordable and easy to use, users now take care of many of their computing needs on their own. People

use word processors, graphics programs and e-mail to accomplish tasks on a daily basis. Using computers gives rise to using networks. Using networks gives rise to information and data sharing. Intranets give rise to sharing information and data sharing in ways that leverages technology to improve productivity.

As intranets become more prevalent throughout DoD, planning for them must become streamlined yet remain efficient to respond to today's rapidly changing environment. While the DoN finalized plans to initiate one of the largest IT projects in its history, the Navy/Marine Corps Intranet (N/MCI), this study was conceived to investigate methods of improving the planning and design process.

B. RESEARCH QUESTIONS

Primary research questions include:

1. What current methods are used to perform intranet requirements analyses?

2. What current methods are used to evaluate intranet infrastructure requirements?

3. What cases of intranet implementation exist within DoN that can be used to validate methodologies?

4. What intranet management practices and tools are available that if applied may result in improved planning procedures?

C. METHODOLOGY

This research effort includes a literature search of books, magazine articles, and other library and Internet information resources describing intranet planning and development issues. A case study of the United States Marine Corps Collaborative Planning Network (USMC CPN) was conducted to provide insight into actual methods used to plan and implement an intranet within an existing network.

Research data collected for the case study was gathered using interviews and site visits with network engineering and administration personnel at the Marine Corps network operations center in Quantico, Virginia. Several telephone interviews and personal interviews were conducted with personnel from the DoN Chief Information Officer's office (DoN CIO), as well as the U.S. Marine Corps Command, Control, Communications, Computers and Intelligence (USMC C4I) office. At the time of the interviews, each location was engaged in planning for the implementation of the N/MCI. This provided keen insight and assistance in validating methods that were discovered during the literature review. Using interview data with the N/MCI as a background, improved methods and procedures for intranet implementation could be discovered in existing literature.

D. THESIS OUTLINE

This thesis consists of five chapters. Chapter II examines methods of conducting a requirements analysis phase of an intranet development project. A three-step

methodology is provided to help planners identify requirements that an intranet will be expected to support. Chapter III examines infrastructure assessment. This chapter provides quantitative methods as well as qualitative guidance on assessing an enterprise network to support the introduction of an intranet. Chapter IV is a case study of the USMC CPN This chapter captures methods used by U.S. Marine network planners and engineers to establish the CPN. Chapter V provides a summary, recommendations and suggestions for further study.

E. EXPECTED BENEFITS OF THIS THESIS

This study provides information and background needed to begin planning an intranet development project. It also serves as a baseline that DoD or DoN organizations can use as a template to develop planning methods for intranets. The material in this thesis is must be covered during planning an intranet project. If these items are not addressed and incorporated by organizations planning an intranet, the task will be much more difficult than if procedures described here are followed.

II. REQUIREMENTS ANALYSIS

A. INTRODUCTION

An intranet is a complex system of systems comprised of computer hardware, software, communications infrastructure, information content, policy and people. Therefore, an intranet project should be approached in the same manner as any system development project. [Ref. 2]

To develop an effective intranet, particular attention must be given to identifying requirements the intranet will support. An initial formal meeting with lead developers, attended by management and user representatives is necessary to capture requirements and performance criteria. [Ref. 2]

Without a clear definition of requirements up front, it will not be possible at project completion to determine effectiveness. Management and users must determine and agree on what information sharing and communications requirements exist, what benefits will increased information sharing bring, and which applications could be web or intranet enabled that will increase productivity. Upon analyzing and answering these and other questions, the project can take shape with effective measurement criteria. This chapter outlines items necessary to consider during the requirements analysis phase of an intranet development project. A three-step methodology to accomplish this and a prototype spreadsheet for capturing costs are introduced.

B. BUILDING THE BUSINESS CASE

Common threads in successful Information Technology (IT) projects are: defined needs, functions new systems will perform, clear overarching vision, and a detailed cost analysis all used to guide development. Defining what an intranet is expected to do will be a foundation for its usefulness. Identifying functions new systems will perform will capture expected capabilities. A vision establishes a view of the end state; it is the description of where the plan is going, and why it must be accomplished. Detailed cost analyses provide information from which decisions can be made concerning allocating funds to support the project. Without defined needs, described functionality, vision, and accurate financial estimates an intranet, or any project for that matter has a lower probability of meeting expectations. [Ref. 9, 10]

1. Need

What must be determined before embarking on development of an intranet is a clearly defined need. A typical need is to connect people with information; and to push information outward. Another is to provide a communication backbone that will support internal software applications used by an organization. Intranets can provide users with access to organization policy documents, personal records, collaborative planning tools, and other enterprise information. A comprehensible need provides a framework for drafting the project mission statement. This document should delineate voids an intranet

will be expected to fill. Determine need or needs you expect an intranet to fill before moving forward with development. [Ref. 9, 10]

2. Functionality

Different from the need for an intranet, are its functions; tasks and operations that an intranet will facilitate. What can an intranet accomplish that current network infrastructure does not? An example of intranet use is sharing internal, enterprise information such as policy or benefit information. Another example is application execution: operating internal client-server software applications between separate departments. Another function is to serve as the medium for video teleconferencing or corporate training programs. Building an intranet may be the only way to execute bandwidth-demanding applications with required speed and reliability necessary to support users.

Intranets are often conceptualized to do things not currently done, using technology to create a leverage point where none existed. This can lead to the creation of a competitive advantage not possible before an intranet. Intranets are sometimes conceived to improve existing processes; in business literature, this is referred to as Business Process Reengineering (BPR). BPR examines and re-designs methods to make them more efficient and streamlined. By operating applications or sharing enterprise information, organizations benefit from centralized management and standardization. With the ability to measure performance of applications and other functionalities of intranets, organizations can determine effectiveness and further leverage technology.

Functionality can be boiled down to understanding what an intranet provides to users. The functionality of an intranet can be anything that an organization desires it to be. The best way to ensure an intranet will have the functionality that organizations desire is to establish a high level vision during the requirements analysis phase.

3. Vision

In the beginning, a vision for an intranet may not reside with senior management. IT experts may understand advantages of creating an intranet and should educate senior leadership about advantages and purposes of intranets. Informing senior leadership and management can expose disadvantages of not having an intranet. Demonstrating how a competitor or peer uses an intranet to gain advantage is one way of revealing drawbacks of not having this tool at your disposal. Once senior management is supportive, enterprise vision for can begin to shape. Vision will also set expectations, which can lead to definable measures for the project. Senior management must become champions of the intranet; the project will take considerable effort and resources to establish. If an organization has a true champion in senior management, opportunity for success is increased. Senior leaders should have or develop a mental model of the intranet and communicate this to managers, developers and users. From this point, the task of transforming vision into reality is left to the information technologist. A clear vision guides the entire process.

4. Cost Analysis

Conducting a cost analysis is necessary to accurately estimate resources necessary to complete the project, and to track return on investment (ROI) calculations. There are many costs of developing an intranet, but the following must be considered during planning: new hardware, software, application development and purchase, communications facilities, personnel, security and client/server license considerations. In addition, a lifecycle management budget should be created for each of the above areas to plan for upgrade and replacement costs. Budgeting resources will prevent surprises when financial demands from each area become reality. Successfully linking intranet development ROI calculations to the bottom line can provide justification management is concerned about.

All items requiring funding will call for a specific line on the budget. A prototype cost calculator spreadsheet is provided in Appendix A to assist in the formulation of a cost analysis. It serves as a starting point to capture items that will require funding for development.

C. ENTERPRISE PLANNING CONSIDERATIONS

Establishing an intranet requires detailed planning. Selecting a platform, web server and application development software should receive attention during the planning phase. During planning, consideration must also be given to two important variables that affect the enterprise: resources, and development schedule. [Ref. 9, 10]

1. Resources

Primary resources that need to be considered are budget, personnel, and existing communication infrastructure.

a. Budget

Allocating funds to develop and produce an intranet is necessary to ensure dollars are available in appropriate amounts when required. It is imperative to understand that setting up an intranet will take significant effort on the part of many individuals to establish. This amount of effort will impact funding for other projects in an organization.

b. Personnel

Staff experience is another important enterprise consideration. It is necessary to determine the experience of available IT staff. It is vital to establish if experienced web developers exist, and what individual commitments to other projects may be. Developing an intranet will absorb a large percentage of knowledgeable personnel that an activity has on hand, as well as require external consulting expertise and effort. [Ref. 8]

c. Communications Infrastructure

Internal communications infrastructure will also require assessment; what is built today will soon be at capacity. Assessing existing communications infrastructure strategically can alleviate sketchy improvised upgrade plans. Establishing strategic intent

for growth can help organizations avoid suddenly finding their communications infrastructure inadequate.

2. Development Schedule

Staff availability, labor budget, and other projects will affect an intranet project schedule. Any of the above variables can contribute to schedule conflicts. Schedule issues such as user availability, test and evaluation periods, and publishing documentation all must be scheduled during the development process. A detailed plan will be essential to communicate the number of tasks requiring schedule de-confliction and integration. Program management tools can help identify and manage critical tasks to avoid schedule conflictions. If critical milestones are not recognized and managed, the project may slip without the development team realizing until it is too late.

D. SCALABILITY

Scalability is the ability of an intranet to meet swiftly growing demands on capacity. Building a scalable system makes future migration to different platforms and applications possible. Scalability can be accomplished by avoiding proprietary lock-in with a singular hardware or software provider, and by building a system with the largest amount of capacity that the budget can support. Planners need to estimate anticipated growth and design systems that are scalable to give an intranet long-term life. A system that is not scalable will become an obstacle to enterprise growth.

E. SECURITY

Security requirements for an intranet are equally as important as security requirements on an organization's network infrastructure. It is sound business practice to prevent entry into the intranet from unauthorized users. It is also essential to prevent unauthorized access to corporate data. Further, it may be important to restrict access to selected areas of an intranet.

Security analysis of intranets should include at a minimum: current security policy validation, value added versus risks of connecting the intranet to the Internet, operating system security, and application level security. If an organization's intranet connects to the Internet, a system of firewalls will be necessary to protect the intranet from unauthorized access. Planners must determine if the intranet must access the Internet, why, and how to properly protect it from unauthorized access.

A good practice to validate systems and software is to have a procedure of checking regularly with the Computer Emergency Response Team (CERT). CERT publishes security regular advisories related to known security holes in commercial products from operating systems to word processors. A practical way to implement this would be monthly validations plan that checks enterprise systems and software against current CERT advisories. [Ref. 9]

Operating systems must only be accessible by trained, authorized personnel. If an intranet's operating system software is not protected, the entire intranet can suffer damage. Unauthorized access can allow users to make changes, which result in disaster.

The use of permissions and access control lists to servers and directories can prevent superfluous tampering of intranet operating software. Determining who should have access to operating system software is imperative to maintain intranet operating system security.

Applications on intranets also require security assessment. Application software residing on hardware throughout an intranet must be kept free from access by anyone other than system administrators. If users have access to application data or program code, system failure could result. A user given uncontrolled access could use proprietary data or code in a harmful manner. Permissions and access control lists can also be used to protect applications from tampering.

F. TYPES OF INTRANETS

There are different types of intranets that accomplish different tasks. An organization may have a specific need for a read only non-interactive intranet, or a hybrid type of intranet where interaction and one-way access is combined.

1. Non-interactive Read Only Intranet

Enterprise information exists in many forms: organizational policies, operational standards, benefits explanations, training and reference material. Typically, this data exists on paper, is difficult to update, republish and is not thoroughly distributed. If documents listed above were available on an organizational intranet, everyone benefits, not just those possessing the most recent hard copy. When changes are made to these and

other documents, it is only necessary to update the electronic version and the latest information is instantly accessible by the entire enterprise. As a read only, non-interactive window to enterprise information, an entire organization can access the latest information.

2. Interactive Intranets

Internal communications and proprietary applications can be carried on an intranet and benefit from increased speed and security. Consider a travel planning application used throughout an organization. This interactive software is capable of making all arrangements for business travel, including billing the correct cost center. Advantages of an application of this type are clear: consolidated input, and labor and cost savings from fewer errors.

Using an intranet as an internal communication backbone where users enter and retrieve data can increase speed and reliability of information exchange, video conferencing, and training applications. Multiple interactive applications can benefit from the two-way communication provided by an intranet: e-mail, logistical planning, database population and replication, personnel management reporting, and others. Keeping organizational communications on an intranet also enhances organizational security by avoiding interaction with outside networks where hackers lurk snooping for information.

G. THREE STEP REQUIREMENTS ANALYSIS METHODOLOGY

There are various ways organizations can begin evaluating and prioritizing requirements that will lead to implementation of an intranet. The method proposed in this thesis is similar to other systems development methodologies but is streamlined and can be thought of like a waterfall, with steps flowing into each other sequentially. [Ref. 1] This method consists of three primary steps each with unique tasks. Each step is discussed in detail in the following order:

- Step One, Business Case Analysis;
- Step Two, Information Needs Evaluation;
- Step Three, Determination of Application Requirements.

Figure 1 depicts this procedure graphically with activities and success factors of each step.

1. Step One - Business Case Analysis

During a business case analysis, organizational goals are evaluated and revised according to current and expected future needs. During this step, an organization clarifies understanding and defines the need for an intranet. The objective: to refine goals and priorities to leverage technology as a catalyst for achievement and process improvement. This is where planners and managers define how an intranet will meet goals and support needs not otherwise being met. During this phase, future needs are identified and clarified. A detailed cost analysis is completed by system planners to accurately estimate

anticipated costs. This estimate will help to identify resources required and will also assist in ROI calculations. Step One is complete when it is clear how an intranet project is expected to contribute value to meeting goals of an organization.

2. Step Two - Information Needs Evaluation

When performing an Information Needs Evaluation, it must be understood that information is different from data. Data can be considered raw facts about people, objects, and events in an organization. Information is data that have been processed and presented in a form suitable for human interpretation.

The first element of the evaluation is to understand the background of an organization. Analyze and document the physical and logical organization with respect to people, processes, and decisions.

Next, planners should observe the current situation to identify information that pertains to a specific function or department. Document what problems exist. Create a functional flow chart of all elements of the organization and corresponding information exchange.

Finally, planners should evaluate current legacy system performance. The intranet planning team should understand what function each system provides. Identify redundancy in processes and information. Planners then determine efficiency, user satisfaction and shortfalls of each system. Identify what needs are not currently being met that an intranet will help resolve. Thoroughly evaluating these systems will help identify which systems will be candidates for replacement by new intranet applications. This step

is complete when the information flow of the organization is clearly understood and documented.

3. Step Three - Determine Application Requirements

After completing step two, it will be evident which applications will require modification, replacement, or addition to the network. When evaluating intranet applications, planners should pay specific attention to license considerations and scalability issues. Strive to understand future needs and avoid locking into another legacy system. Evaluate interoperability that may be required throughout an organization.

H. SUMMARY

This chapter has outlined a method for completing a requirements analysis phase of an intranet development project. Key factors in the beginning of an intranet project are a defined need, documented functionality, clear vision, and detailed cost analysis. When planning an intranet, there are many factors to consider, but three variables must be planned with the enterprise in mind; budget, personnel, and communications infrastructure. Scalability is addressed as an enabler to future growth. Security is addressed to impress the need for comprehensive security policies and network protection. Different types of intranets are discussed to differentiate the differences between levels of inter-activity. A three-step method of intranet systems development is proposed along with a prototype spreadsheet for initiating intranet development.

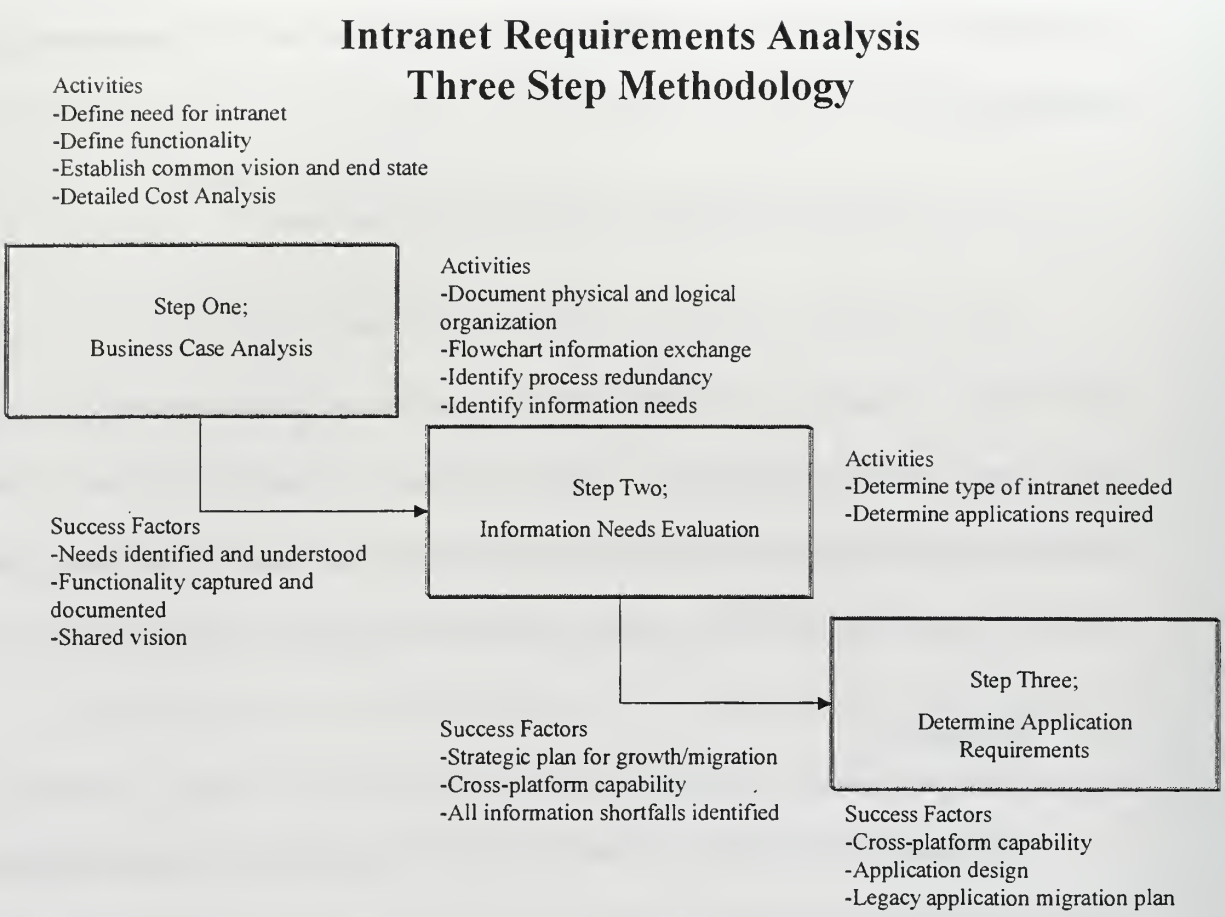

Figure 1. Intranet Requirements Analysis Three Step Methodology.

III. INFRASTRUCTURE ASSESSMENT

A. INTRODUCTION

This chapter describes items that are part of an organization's network infrastructure. Infrastructure consists of inter-related items that make up an organization's network. More than servers, personal computers, networks, and communication devices, it includes people and their responsibilities, training, security and the architecture that bonds them together. Infrastructure assessment is the task of analytically evaluating all elements that make up an intranet infrastructure, including determining future needs. It determines the suitability of your current infrastructure as an intranet platform. This chapter discusses elements of infrastructure that an organization contemplating an intranet development project would be wise to assess and recommends a method of carrying out this procedure.

B. ELEMENTS OF INFRASTRUCTURE

Many elements that are part of network infrastructure are obvious to information technology (IT) professionals and managers. These items make up the backbone of a network: computer hardware, software, communications, and security devices. Less obvious elements are people, responsibilities and skills. Each element has unique characteristics that need to be considered independently as well as how they interact with other elements of infrastructure.

C. COMPUTER HARDWARE

Computer hardware is defined here as servers (of all types) and personal computers (PCs). It is important to assess the level of operational capability of servers and PCs. These items contribute more than any other items of hardware to the daily operation of activities that take place on an intranet. To accurately assess where an organization stands with respect to performance capability an analytical quantitative assessment must be completed to capture current capabilities. This assessment will also be the starting point for determining future requirements.

1. Servers

The primary hardware consideration of a network infrastructure assessment are the servers that store and process information. One method of assessing overall performance is benchmark tests. A benchmark test is an application that tests a servers' ability to respond to multiple types and frequencies of queries simultaneously. The test provides response time ratings of the servers performance against a standard used in the benchmark software. Benchmark evaluations provide concrete and tangible data. However, during assessment, evaluate these results with other information.

Another method of measurement is conducting a survey of the types of servers on hand and recording capabilities of each in a table. When assessing servers, it is important to measure random access memory (memory), hard disk capacity and processing power capabilities of each server. Each item is assigned a weight from which scores for each

server are calculated and compared against one another. Table 1 is an example of a method that can be used in conjunction with benchmark tests for overall evaluation.

Server Name	Memory	HD Capacity	Processor Speed	Misc. (hot swappable HD) – Space open for upgrade	Total Score
Hue City	3	1	2	2	8
Iwo Jima	1	2	2	0	5
Key:	< 64MB = 1 64-128MB = 2 128-256MB = 3	< 10GB = 1 10-20GB = 2 20-24GB =3	<450MHz = 1 450-600Mhz = 2 > 600MHz = 3	Misc. Swap HD = 2 Upgdbl HD = 2 Upgdbl RAM = 2	

Table 1. Server Evaluation and Score.

Following quantitative measurements, qualitative evaluations need to be conducted for these and other items measured with numbers. Level of usage will have to be considered as well as potential usage upon implementation of an intranet. Age of the server is also an important consideration. How will the anticipated growths of the intranet affect the server? How long can current hardware provide the level of quality of service desired? What is the migration and acquisition strategy to sustain network performance?

Other considerations are the types of servers required to operate specific functions on an intranet. Types of servers possibly required are:

- Domain Name Server (DNS) able to convert English names of servers to IP addresses used to transit the intranet or Internet;

- Hypertext Transport Protocol (HTTP) server provides Hypertext Markup Language (HTML) pages to web browsers;
- Proxy Server allows access to the Internet from the intranet;
- Simple Mail Transfer Protocol (SMTP) server necessary for e-mail.

These are some of the items to consider when assessing server hardware. Computer processing power currently has about an 18-month life span before being replaced by the newest technology [Ref 12]. With technology becoming increasingly affordable every month, it is necessary to determine priorities of future system performance so a smooth, continuous upgrade plan can be executed.

2. Personal Computers

Personal computers make up the other large portion of infrastructure and require a similar type of evaluation. Processing power, memory, hard disk capacity, and multi-media devices need to be assessed for each PC. Using Table 1 modified for PC evaluation will help planners complete this task. After measuring existing PCs and obtaining a quantifiable result, qualitative judgment must be applied with respect to goals and ambitions of an organization. For example, if an organization desires to operate distance learning or other types of training applications PCs will require necessary processing power and multi-media capability to perform media-rich training applications.

Before collecting quantitative data in each of the above surveys, organizations should devise a method to rank systems after scores are obtained. It is possible to use the

scoring data to rank systems in order of replacement or upgrade priority. After the data are gathered, organizations will have a better understanding of the state of the hardware inside their infrastructure.

D. SOFTWARE

In any organization, there are different types of software used in many tasks. For example, office production software, rapid application development tools, database applications, and computer aided drafting software. A software assessment should determine every type of application used, along with corresponding seat cost, which is defined as the dollar amount required provide software on every terminal where it is required. The most critical types of software requiring assessment are server and browser applications.

1. Web Server Software

During a server software assessment, it is necessary to account for each type of server and its operating system software. Servers combined with their operating system software are known as platforms, of which the major types are Macintosh Power PC, Unix, Windows NT and Linux. Although interoperability is shared among these platforms, planners must understand what types of platforms exist within their infrastructure.

Operating system, file system, and network system are standard software components of each server on a network. These systems in turn support every function a

server performs. Standardization in each of the above areas makes network management and future expansion easier. Conversely, organizations should avoid lock-in with a single provider. Choosing a single vendor for all functionalities may be tempting for ease of use and procurement. However, this strategy can produce problems if a vendor cannot support future needs.

During assessment, interoperability and scalability of server components must be considered. Using a survey method similar to Table 1, planners can gain an understanding of the level of interoperability throughout a network. Table 2. Server Software Assessment, is an example of how to record server software assessment data.

Item	Server	Operating System		Network Op. System		Virus Software	
Number	Name	NT	Unix	TCP/IP	Novell	McAfee	Norton
1	Iwo Jima	X		X		X	
2	Hue City		X	X			X
3	Tarawa		X	X			X
4	Chosin	X		X			X
5	Guadalcanal	X		X		X	
Totals		3	2	5	0	2	3

Table 2. Server Software Assessment.

2. Browser Software

Browser software is the application that provides the interface for information display via an intranet. It is through browser capabilities that applications come to life. Browsers offer enhanced capabilities through plug-ins; small application upgrades that allow browsers to perform advanced functions usually related to media display

capabilities. The browser is the container through which users manipulate and interact with applications. Throughout an organization, it is not necessary to standardize web browser software since the market leaders of these applications are equally capable. What is necessary is that every PC required to interact with information on an intranet has web browser software installed and functioning.

E. INFRASTRUCTURE COMMUNICATIONS

This thesis assumes that organizations considering implementing an intranet have an existing network. The discussion below is intended to provide planning guidance on issues necessary for a successful implementation of an intranet. The Consultative Committee for International Telegraphy and Telephony (CCITT) defines the task of network planning as follows:

> Network planning is the continual interactive process of
>
> - monitoring the current network characteristics;
> - understanding environmental constraints/considerations;
> - forecasting future needs and technology;
> - creating the most appropriate, consistent and coordinated plans on a long, medium and short-term basis;
> - modifying plans based on results of actual implementations;
>
> in order to provide ongoing cost-effective and timely communication service to users. [Ref. 4]

This definition makes it clear that communications system planning is an iterative, interactive process. Communications system planning relates to the physical and logical network structure. Organizational and operational aspects affect how tasks are distributed throughout an organization. Assessments need to complete examinations of site communication needs, cable path analysis, and a quantitative assessment of communications capabilities. [Ref. 4]

1. Organizational Structure and Levels

In most organizations, different departments process different types of data and have different needs with respect to processing power, back up, and storage capability. These requirements have an affect on the distribution of computer related items such as PC's, servers, and other peripherals. The distribution of assets affects the network in terms of types and amounts of traffic on the network. [Ref. 4]

Organizations are usually separated into sub-areas based on spatial distribution or functionality. These subdivisions can produce further fragmentation each with level-specific functions. For example, in a university environment such as the Naval Postgraduate School, levels could be separated as follows:

- Level 1: user workstations (student PC labs)
- Level 2: decentralized shared services (network servers assigned to students and departments)
- Level 3: central servers and databases (department servers and databases)

- Level 4: high-performance computers (large mainframes)

Each level is different with respect to types of computers, and corresponding communication requirements in terms of:

- nature and frequency of data transfer
- nature of data exchanged (signals, dialogue, files, reports, graphics)
- extent of real-time requirements
- device interface

All levels of a network have different hardware interfaces, transmission rates, and protocols that require assessment during planning. It is necessary to evaluate the above variables to ensure that communications networks can to meet future requirements for increased capacity and functionality.

Communications infrastructures need to be planned with modularity in mind. This allows administrators and engineers to make alterations during the lifetime of the network. Understanding an organization with respect to data-processing types and functionalities is a useful way to begin the assessment of an existing network. [Ref. 4]

2. Site Communication Needs Assessment

The objective of a site communications needs assessment is to derive diagrams similar to Figure 2, the Naval Postgraduate School Communication Backbone. Information gathered is used to analyze the spatial distribution of organizational groups,

levels, and sub-levels. Data obtained can be used to make network planning decisions such as:

- choice of topology;
- location of servers and workstations;
- cabling structure;
- arrangement of security devices;
- location of switching devices, repeaters, hubs, and bridges;
- gateways to the Internet or extranets.

Following the communications needs assessment; a cable path assessment must be completed. [Ref. 4] [Ref. 5]

3. Cable Path Assessment

Considering required bandwidth and anticipated growth, existing cables must be assessed with respect to their ability to meet expected increases in usage brought on by an intranet. Cable types, and their electrical and mechanical characteristics must be determined. Physical restrictions with respect to rooms for network components, position of cable runs, locations for routers, bridges, hubs and distances involved needs to be measured. It is necessary to evaluate electromagnetic interference and climatic conditions that could lead to shielding requirements or establishing alternate paths. Understanding restrictions will assist in determining what can and cannot be intranet implementation. Upon completion, a cable path analysis will provide the basis for estimating cable costs and will assist in quantitative assessment of network needs. [Ref. 4]

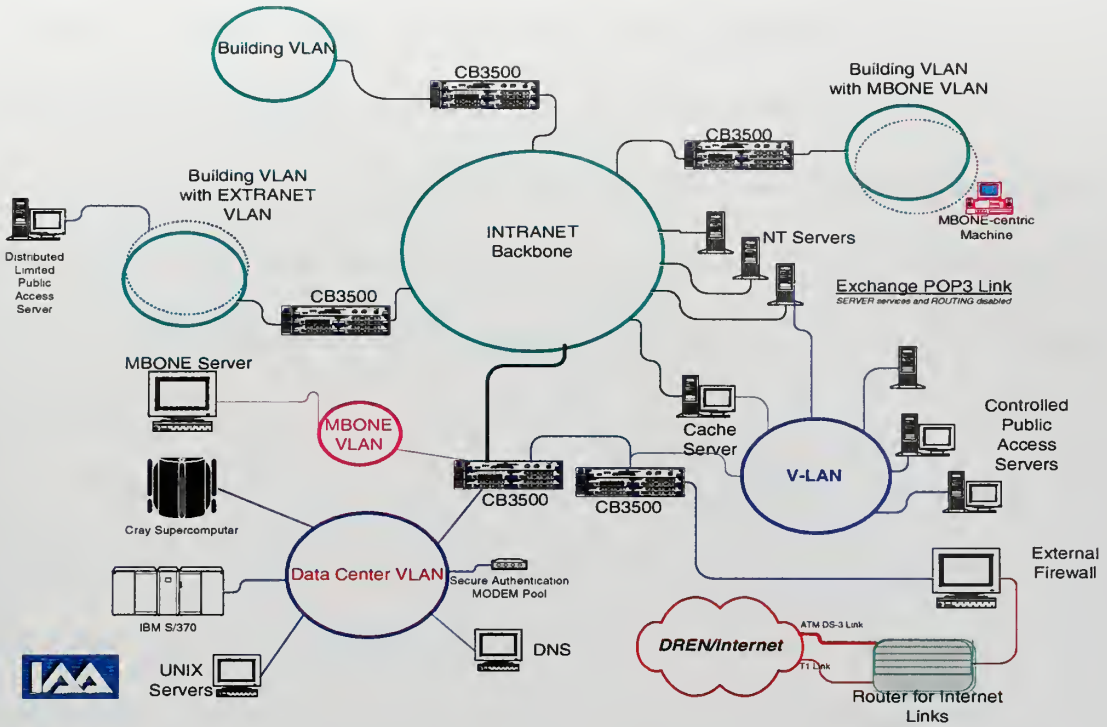

Figure 2. Naval Postgraduate School Communications Backbone.

4. Quantitative Assessment of Capabilities

In order to plan for intranet usage on an existing network infrastructure, it is necessary to assess different types of data that will transit the network. Different types of data impose different bandwidth requirements on the network. For example, on-line transmission of voice requires a special frequency band and a low delay; however, because of the physiological properties of the ear and speech redundancy, reliability and error rate requirements are lower than those for data are. [Ref. 4]

Transaction characteristics encompass volume and time related information of interactions of communications relationships over computer networks. These include: the number of users, connection type, operating mode, interaction frequency, type and

volume of information per interaction. Transaction characteristics vary for data entry, batch applications, information retrieval and file transfer. [Ref. 4]

Transaction characteristics can be specified using approximate values. Using a list of devices and applications, an attempt can be made to estimate typical application specific message lengths. Transfer rates for relevant pairs of users and applications can be determined for average and peak loads.

Measurements that are more detailed can be obtained by using electronic tools that measure actual traffic load on networks. These tools also have the ability to subject networks to artificial loads and measure performance. Data obtained from transaction transfer rates and network evaluation tools can be used to estimate traffic loads and determine requirements for increased bandwidth or additional cable path information. [Ref. 4]

F. SECURITY ASSESSMENT

Security assessment begins by completing a risk analysis of the current infrastructure and determining potential areas for harm. A computer network risk analysis is an evaluation of a system and the associated risks of doing or not doing something. When a risk analysis of a particular system is completed, security plans and policies can be put into action. [Ref. 7]

1. Risk Analysis

A risk analysis is a series of steps taken to evaluate the security of a given network in an organized, formal process borrowed from practices in management. Specific steps of an analysis can be modified to meet organizational needs. During this analysis, confidentiality, integrity, and availability are the major concerns.

Confidentiality means that a system or asset is only accessible by authorized parties. Integrity means assets can only be modified by authorized parties. Availability means assets are accessible to authorized parties. Availability is sometimes known by its opposite, denial of service. An example of the steps involved in a risk analysis are explained below and can be used as a starting point. The basic steps are: [Ref. 7]

- identify assets;
- determine vulnerabilities;
- estimate likelihood of exploitation;
- compute expected annual loss;
- survey applicable protection methods and their costs;
- project annual savings of control.

a. Identify Assets

The first step is to identify assets of a computing system or intranet. These assets are collected into categories and listed as in Table 3. A risk analysis starts with an

inventory of the system. Questions regarding vulnerabilities considered during an analysis are: [Ref. 7]

- What are the effects of unintentional errors?
- What are the effects of willfully malicious insiders?
- What are the effects of outsiders?
- What are the effects of natural disasters?

Asset	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
Documentation			
Supplies			

Table 3. Assets and Security Properties.

b. Identify Vulnerabilities of Assets

This step is qualitative in nature and requires planners to make assessments based on judgment and experience. Vulnerability is any situation that could cause a loss in confidentiality, integrity, or availability of the assets that support an intranet. [Ref. 7]

c. Predict Likelihood of Occurrence

Prediction involves determining how often each asset will be exploited. It may be impossible to predict the likelihood of occurrence of some events. However, it is more likely that planners will need to estimate within a given frame of reference. Table 4

is an example of ratings of likelihood of occurrence. Incidents that occur more often are given a higher rating. Higher ratings equate to more detrimental situations. [Ref. 7]

Frequency	**Rating**
More than once a day	10
Once a day	9
Once every three days	8
Once a week	7
Once in two weeks	6
Once a month	5
Once every four months	4
Once a year	3
Once every three years	2
Less than once in three years	1

Table 4. Ratings of Likelihood.

d. Compute Annual Loss Expectancy

Computing the cost of an incident is the next step of performing a risk analysis. This value may be difficult to determine, or it may be straightforward. Determining the cost of a server or computer is easy and can be derived from purchase records or current replacement costs. However, determining the cost of losses from lack of access to a system is more difficult. If an intranet is unavailable, causing tasks to be delayed, there can be serious consequences. Attaching dollar values to these failures can be obtained by estimating value based on the following questions:

- What is the value of access to data or programs? How much would it cost to have the function performed elsewhere?

- What is the value to someone else of access to data or programs? How much would a competitor pay for access?
- What problems would arise from loss of data? Could it be replaced? Could it be reconstructed? With what amount of work?

Once the cost of an incident is estimated, it is multiplied by the expected number of occurrences per year. This produces an estimate of the yearly loss. This loss is called the Annual Loss Expectancy (ALE). For example, one incident may be expected to cost $15,000, and have a frequency of occurrence of 2 times per year while another event may cost is $1000000 and may have frequency of once every 4 years (0.25) times per year. The ALE of the first incident is $30,000, while the ALE of the second is $250,000.

e. Evaluate New Methods

The computations above would be based on the status of a network infrastructure with current protection measures and methods in place. Therefore, cost estimates provide information on the current situation. If costs of expected losses are unacceptably high, new methods or protection measures need to be evaluated and implemented. [Ref. 7]

One way to identify new methods of protection is to evaluate each on a per-exposure basis. For example, a risk of data loss could be covered by periodic back-ups, access controls and redundant storage devices. Each of the measures would be evaluated with respect to cost and effectiveness to prevent data loss. When cost of data

loss is obtained, it is necessary to project the savings provided by protection measures against the cost of not implementing them.

f. Project Savings

During this step, the cost or savings from implementing a new control are computed to determine the effective cost. The effective cost is the cost of the control minus any reduction in ALE from using the control. In order to complete this step, risks must be analyzed and their associated cost estimated. Following this, a determination of the effectiveness of the protection measure is estimated. The next step is to determine the expected annual costs of losses and controls. Subtracting the cost of the protection measure from the cost of recovering from an incident produces the effective cost of the protection measure. This figure is used to determine the cost or savings derived from implementing the protection measure. An example of this step is outlined in Table 5. [Ref. 7.]

Item	Amount
Risk: disclosure of confidential data.	
Cost to reconstruct correct data: $1000000@10% likelihood per year	$100,000
Effectiveness of access control software: 60%	-$60,000
Cost of access control software	+$25,000
Expected annual costs due To loss and controls $100,000 - $60,000 + $25,000	$65,000
Savings: $100,000 - $65,000	$35,000

Table 5. Justification of Access Control Software.

2. Benefits of Risk Analysis

Using risk analysis will help planners understand security risks associated with developing an intranet. The benefits of risk analysis are to:

- improve awareness;
- identify assets, vulnerabilities, and controls;
- provide basis for decisions;
- justify expenditures for security.

A risk analysis will force a systematic study of the exposures associated with an intranet or any computing system. Discussion generated during a risk analysis assessment will improve overall awareness of the need for security measures and will contribute to creating or improving security plans and policies.

G. PERSONNEL

Developing an intranet requires specific information technology (IT) talents and backgrounds. The staff that supports an intranet must have knowledge of network administration, security, communications, and web development.

1. Network Administrator

The network administrator is responsible for the overall performance of the intranet. A network administrator must be able to manage an intranet to provide reliability and high quality service.

2. Security Administrator

Security of the intranet encompasses enforcing general security policy, as well as monitoring internal security and preventing outside attacks. Tasks of the security manager should not be left as collateral duty for someone else on the IT staff.

3. Web Publisher

The web publisher has the final responsibility for content published to the intranet. Departments may have content developers and site designers, but should not have the authorization to publish material directly to an intranet. Lack of an approval procedure will make establishing consistency and clarity on an intranet difficult.

H. INFRASTRUCTURE ASSESSMENT METHODOLOGY

The methodology of infrastructure assessment put forth in this chapter is a five-step method with each step described below and graphically shown in Figure 3.

1. Step One - Hardware Assessment

During this step an assessment of an organization's computing hardware is conducted. All servers and PC's are assessed with the following measurements taken: quantities of servers and PC's, types (brand names), and characteristics with respect to processing power, memory, and disk capacity. This step is complete when a reliable inventory exists for all assets. The amount of detail in data reports can be filtered as they are passed to higher planning levels. Information that is more detailed is necessary at

lower levels of management to manage accountability, interoperability, and upgrade priority concerns.

2. Step Two - Software Assessment

During this step, the only types of software assessed are server software and browser software. This is necessary so planners have a detailed understanding of capabilities and interoperability issues to support an intranet. Completing this step will expose the level of standardization in an organization. This step concludes with a reliable inventory of server and browser software types, and an evaluation of license arrangements.

3. Step Three - Communications Assessment

Activities in this step are analytical and consist of network testing, measurement and evaluation. A site communication needs assessment is completed that outlines requirements of various locations in an organization. Cable path analyses are conducted to determine efficient cabling plans and cost estimates. Quantitative assessment of existing communications capabilities is also completed. This step is complete when the following documents are created: a communication backbone diagram and a cable cost estimate.

4. Step Four - Security Assessment

There is one primary activity during this step, the security risk assessment. This is a six-step procedure that examines all aspects of intranet and computing system security

issues. This step is complete when all vulnerabilities are identified, and likelihood of occurrences are estimated. Information from this step will be important in formulating the security plan and policy.

5. Step Five - Personnel Assessment

Step five is completed by issuing surveys and interviewing personnel to determine skills and abilities. This step will also help identify personnel needs for recruiting and replacement. This step concludes with the identification and list of the intranet development team.

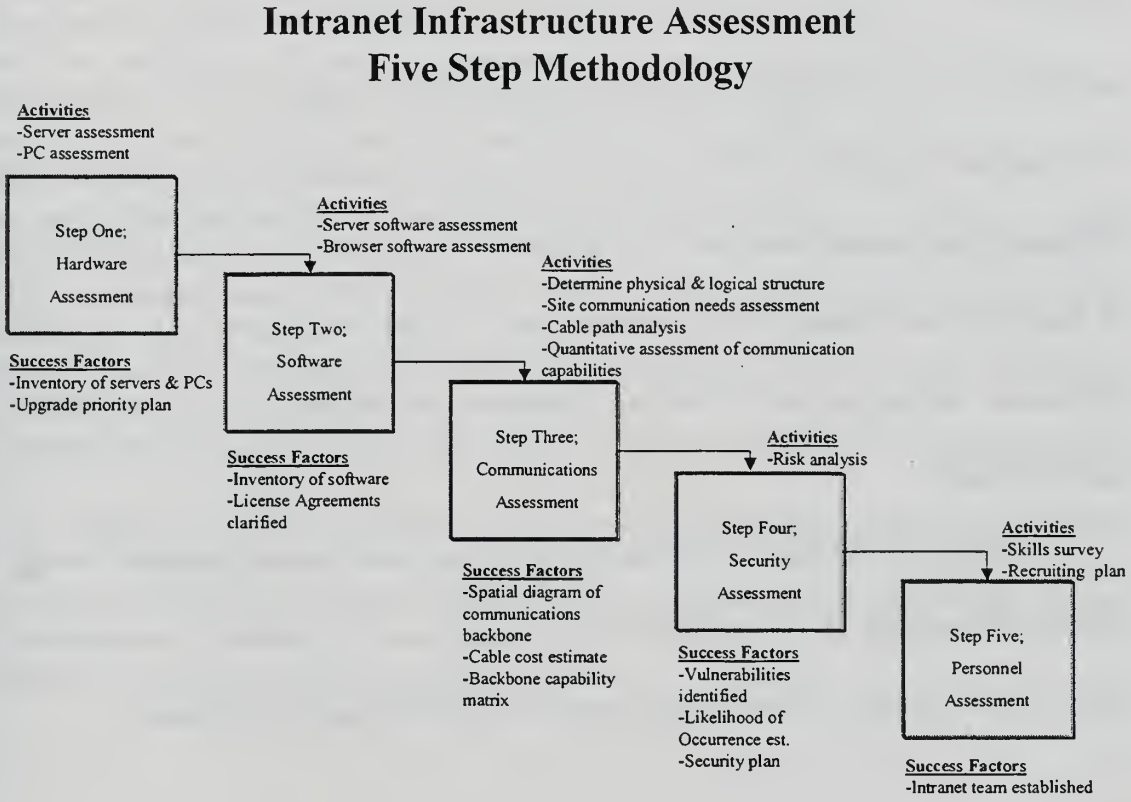

Figure 3. Intranet Infrastructure Assessment Five Step Methodology.

I. SUMMARY

This chapter has outlined a method for completing an infrastructure assessment portion of an intranet development project. Key factors requiring assessment are hardware, software, communications, security and personnel that will support the intranet. Quantitative as well as qualitative measurements are made against each of the above items. The importance of knowing exactly what is present within an enterprise can assist in determining what will be needed in the future.

The methods presented in this thesis provide a means to survey and capture the analytical data needed to assess the status of hardware and software throughout an organization. Measurement of network communications capacity and performance using the methods described in this chapter can provide information that can be used to efficiently plan communications network needs. The discussion of personnel is included to highlight this element of an infrastructure. Without the correct mix of personnel possessing the proper mix of skills, experience, an intranet project can become an untamed beast.

A five-step method is proposed as a way to guide intranet planners through the process of assessing the infrastructure of an enterprise. This method is streamlined but can be scaled to meet a more detailed approach to planning and development.

IV. CASE STUDY OF THE UNITED STATES MARINE CORPS COLLABORATIVE PLANNING NETWORK

A. INTRODUCTION

This chapter augments the comprehension of requirements analysis and infrastructure assessment methodologies with a case study in network operations. The United States Marine Corps manages its worldwide data communications network from a main operations center in Quantico, Virginia. The use of this network has grown substantially over the last seven years. Because of this growth, network engineers and users have seen the performance of their network decrease. Multiple deficiencies began to become daily challenges for network administrators and engineers. Primary among them were traffic flow analysis, and bandwidth management. Currently, administrators lack the ability to accurately analyze traffic content with the level of detail required to thoroughly understand what is transiting the network. Also needed was an ability to manage bandwidth to best support users who require increased bandwidth to operate network centric applications. With a steadily crowding network and future planning that indicated even greater reliance on network centric tools, managers and leaders began to seek alternatives to augment existing capability.

B. USMC NETWORK MANAGEMENT OPERATIONS

The network management philosophy of the Marine Corps is one of central enterprise network management. The reasons for this are straightforward: to increase security, control configuration management, enforce policy, and distribute network wide changes easily. This strategy is accomplished and implemented around the clock, three hundred and sixty-five days a year by the Marine Information Telecommunications Network Operations Center (MITNOC), as it manages the network infrastructure that supports the Marine Corps known as the Marine Corps Enterprise Network (MCEN).

1. MITNOC

The MITNOC is located in Quantico, Virginia and provides centralized enterprise network management for the entire Marine Corps. The MITNOC provides continuous, secure, global communications and management of the MCEN.

2. MCEN

MCEN is the Marine Corps global enterprise network that supports all data communications for Marine forces worldwide to affect information exchange across the global information grid (GIG). It is composed of Defense Information Systems Network (DISN) only connections consisting of 32 unclassified and 19 classified points of entry spanning from Europe to Korea centrally managed by the MITNOC. Figure 4 graphically depicts the MCEN.

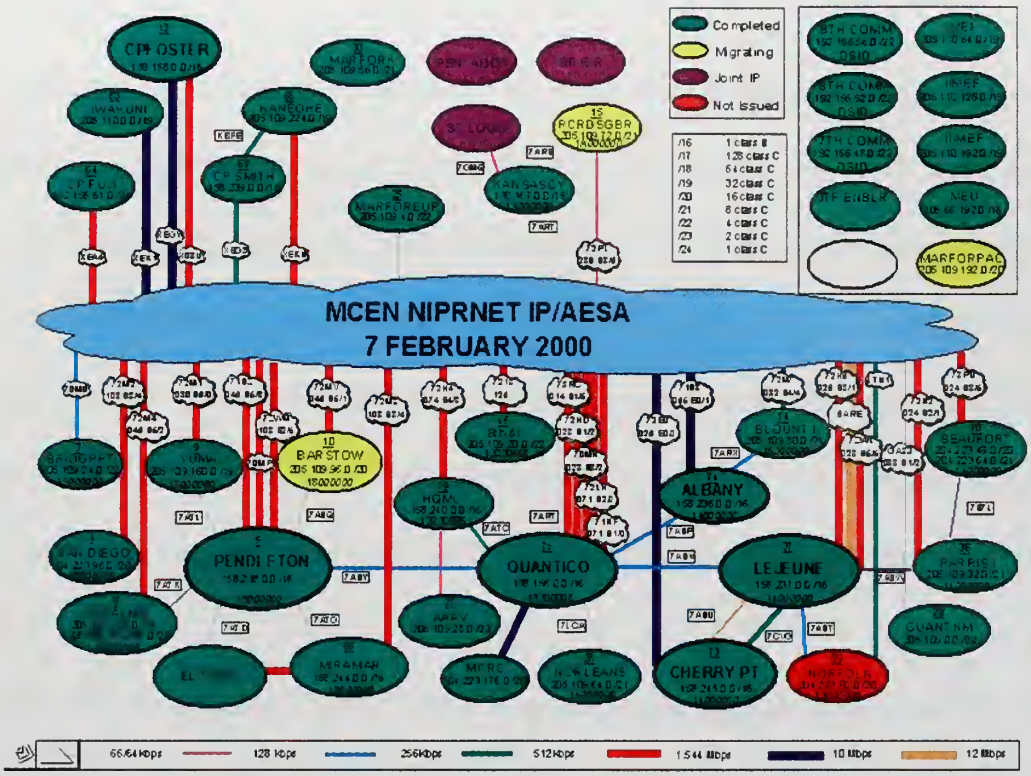

Figure 4. The Marine Corps Enterprise Network.

C. MISSION NEED DRIVERS FOR ESTABLISHING A COLLABORATIVE PLANNING NETWORK

All MCEN circuits feed into one of two distinct areas of the DISN. These two areas support unclassified and classified traffic separately. The unclassified network is known as the Non-Classified Internet Protocol Routed Network (NIPRNET). The classified network is known as the Secure Internet Protocol Routed Network (SIPRNET). The MITNOC does not have direct control of these circuits with respect to dynamic bandwidth management or traffic flow analysis. All requests for circuit configuration

must be submitted to the Defense Information Systems Agency (DISA) in writing and await DISA approval.

Because of increased use of the NIPRNET for official traffic and the migration of many legacy non-internet protocol (IP) applications such as the Marine Corps Total Force System (MCTFS), the Supported Activities Supply System (SASSY), and the Logistics Management Information System (LMIS); the NIPRNET has become congested. It is routine for users to wait for a minute or more for web pages to load, and even longer for files attached to e-mails to download onto personal computers (PCs). This congestion has led to decreased quality of service for users who must access applications on distant mainframes.

Although no specific metrics exist capturing this degradation of service in quantitative detail, MITNOC administrators described case after case of on-site visits with users that attempt to log into remote mainframes but never gain access. In Quantico, the Human Resources Department suffered from this when a server requiring daily access was moved to a regional site in Norfolk, VA. Since the move, the department has slowed to a crawl as they wait for extended periods to log in. They also must deal with connections being terminated in the middle of transactions. Therefore, the problem is only qualitatively measurable by the number of complaints from unhappy users and the experience of MITNOC administrators.

Since the MITNOC cannot manage traffic flow on DISN circuits, there is no way to distinguish between official traffic and wasteful Internet surfing. Another

immeasurable variable is how much Internet surfing is official, and how much is not. The only way this can be monitored is through traffic flow analyzers known as sniffers.

Sniffers normally exist at the base post or station level and analyze all traffic flowing into and out of the local network. Sniffers are usually configured to search for key words, and IP addresses associated with sites pornographic in nature. Sniffers alert administrators when data packets are detected that contain information not in line with Internet usage policies. Technology exists to pinpoint the exact PC, user logged in, and time of occurrence.

However, this does not solve the problem of proper use of the Internet. Therefore, it is up to local managers to supervise Internet usage. This is normally done by limiting access to the Internet to users with legitimate need, or PCs in the workplace that are easily monitored. Internet surfing can be and is official in nature when done properly and in accordance with standing policies.

The final issue is bandwidth management; there is no way for the MITNOC to dynamically allocate network bandwidth when and where needed. For example, if tow commands desire to conduct a video teleconference, they must notify MITNOC in advance, giving MITNOC time to coordinate with DISA for additional circuit bandwidth necessary to conduct a VTC with acceptable performance. Currently, DISA requires a thirty-day notice to make any circuit modifications. This is clearly not acceptable to anyone trying to leverage the power of network-centric tools to their advantage.

Each of the above issues has contributed to frustrated users who began to seek other means of network connectivity. Administrators and network engineers at MITNOC

must approve all requests for additional circuits installed anywhere in MCEN, or on any base post or station in the Marine Corps. With network performance gradually worsening, users began to submit requests to MITNOC for dedicated circuits to operate applications between disparate locations. The example given during interviews was the need for dedicated circuits to support applications being tested and fielded by Marine Corps System Command.

The increased frequency of these requests from users throughout the Marine Corps led MITNOC engineers to seek an answer to the problem of network performance. This was the beginning of planning of the CPN.

D. METHODOLOGY

A method for solving this quality of service problem starts with identifying a working network model and determining what aspects could be applied to a solution. A working model was found in the Tactical Data Network (TDN). The second step is to design and build a network that will not share the same circuit path as current network traffic. The primary requirement for a separate network is bandwidth availability; there simply is not enough on the current network. Planning for future requirements emphasizes that new applications will require increased bandwidth; it will no longer be sufficient to share the same network infrastructure as existing traffic.

1. Tactical Data Network Model

The Tactical Data Network (TDN) is designed to provide integrated data communications for tactical systems. The theory behind the architecture of TDN is that a commander should be able to direct and control a network just as any other supporting asset supporting the mission. It is designed to be flexible, with change in mind, recognizing that requirements are fluid in battle and demand network adaptability. Figure 5 depicts the current TDN. From the Marine Forces (MARFOR) TDN gateway and below, the MARFOR commander controls the network to support the mission. The same philosophy applies to the design behind the CPN. From the MITNOC, all network management is controlled to support the mission. Currently, this is out of the hands of MITNOC personnel and in the hands of DISA personnel. The CPN is designed to support a "train as you fight" frame of mind.

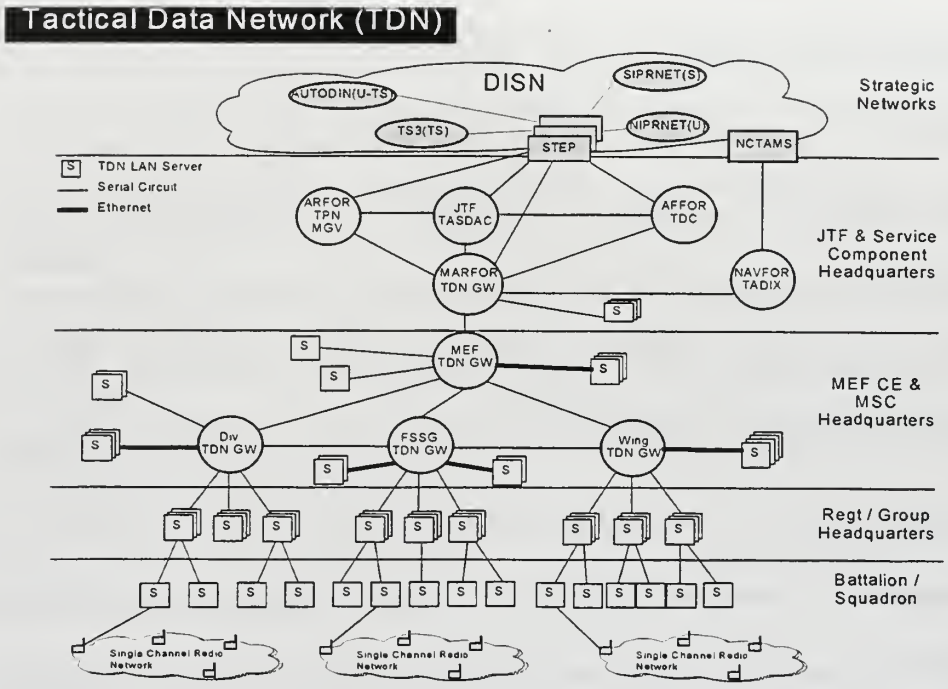

Figure 5. The Tactical Data Network.

E. REQUIREMENTS ANALYSIS

The Collaborative Planning Network (CPN) initiative did not begin with a formal requirements analysis procedure. As the case in many IT projects, defining requirements was less than straightforward, but problem identification was obvious; the current system was broken and required attention. Without a remedy, network performance could only deteriorate. The primary requirements of the CPN would be to enable dataflow management, traffic analysis, and dynamic bandwidth allocation by MITNOC

administrators. Enabling data flow management and traffic analysis will allow the MITNOC to monitor and measure traffic flow resulting in more efficient and responsive network performance. Dynamic bandwidth allocation allows MITNOC personnel to manage bandwidth to support users and applications when and where required.

The requirement for dynamic management of dedicated network circuits is the primary objective of CPN. Currently, many daily use applications such as the Marine Corps Total Force System (MCTFS) run on remote mainframes and other distributed computing resources. These applications routinely time out, or execute so slowly that it is cumbersome and inefficient to use them. Users stare at logon screens for minutes before gaining access to remote applications. Once logged on, manipulating data can be even slower, grinding production to a standstill. The need for dedicated circuits has become so obvious that users have begun to submit requests to MITNOC to purchase circuits separate from MCEN.

1. Dynamic Bandwidth Management

Network administrators are aware that networks are not always tasked to capacity. There are peak periods of use, and off peak periods of low to moderate activity. Many applications do not require large amounts of bandwidth to operate efficiently. Therefore, it makes sense to dynamically manage bandwidth and distribute more to those that need it when they need it. This capability does not exist within the current MCEN architecture. The current process for submitting requests to DISA to change bandwidth allocation is slow and inefficient. The process begins with by submitting a Request for Service (RFS)

from the customer. Following the receipt of this, DISA will assign a Telephone Service Request (TSR) for the request. Following this, DISA will assign a Telephone Service Order (TSO). This process can take up to a year or more to complete. This is unacceptable. Network engineers and managers need the ability to dynamically allocate bandwidth at all times of the day to users who require it. Without this capability, the network is limits potential leverage. When skilled administrators execute this practice, all users enjoy faster access to web pages, quicker downloads and other aspects of increased network efficiency. This can all be accomplished with minimal workload increase to current network administrators. MITNOC network administrators and engineers have designed a system that will integrate smoothly into existing manpower levels through automation and streamlining of current procedures.

2. Traffic Flow Analysis

Traffic flow analysis is an exercise of analyzing network traffic to assess many variables. Commonly, network traffic is monitored for usage to see when networks are at peak use versus off-peak loads. Traffic analysis software and techniques also allow administrators to see what types of traffic are on a network. Analysis tools enable administrators evaluate data packets for payload, and address information. Assessing network traffic for content is a complex, time consuming process. With the existing architecture of MCEN, it is nearly impossible to analyze network traffic content. It is not possible, without a difficult, time-consuming procedure of polling numerous routers and databases to determine which traffic is "official," and which is surfing. This is not to say

that that surfing is not official or at times necessary. However, the increase in IP traffic has contributed to an overall decrease in network performance. The increased traffic has aggravated the issue of application timeout and poor network performance. What MITNOC administrators require is a way to analyze what type of traffic is on the network, where it is going, and what time it is commonly found on the network. For example, a pay clerk at Camp Lejeune requires access to information located on a remote mainframe in Kansas City. At the same time, another user may be conducting research for an upcoming exercise by searching the Internet for pertinent information. Both types of network use are official; but the load on the network created by surfing can have a negative effect on querying data on remote mainframes. With all users sharing the same path, the DISN NIPRNET, network traffic has increased to the point that a consistently low quality of service exists. In the above example, surfing can be considered "other" network traffic, and the pay clerk's traffic can be considered "USMC only" traffic. Without a means to analyze network and distinguish between the two types of traffic flow, it is nearly impossible to understand what is happening on a network, when, where and why.

3. Ability to Support Future Application Development and Research

With the arrival of network based applications it is easier than ever before to collaborate and improve planning and execution processes across geographically dispersed locations. With units distributed around the globe, the Marine Corps can leverage network technology to improve information flow, report current operational

status and use tools that support collaborative planning and management. Currently, researchers, developers and vendors are bringing many network centric software applications to market. Therefore, it is necessary for network engineers and managers to have the ability to support new application testing and development. With the current architecture of MCEN, personnel at the MITNOC are unable to support this requirement at a level acceptable to users. Marine Corps System Command (MARCORSYSCOM) is also located aboard Quantico, VA. MARCORSYSCOM Marines plan, design and test many software applications that will eventually be fielded. Within the last four years there has been and increase in MARCORSYSCOM planning and procuring network centric software applications without involving MTINOC personnel. As applications that require larger amounts of bandwidth than were available on MCEN were fielded, problems soon followed. As a result, frustrated users attempted to build their own networks without approval from MITNOC. MITNOC was the last to find out that they were not providing adequate support. Without a robust global network that can flex to meet varying needs of users, the ability to press forward with development and fielding of future applications is hampered. The CPN design and architecture allows network administrators to support users who require dynamic service.

F. INFRASTRUCTURE ASSESSMENT

MITNOC engineers and managers knew that the existing infrastructure of MCEN would not support requirements established for the CPN. The first step of accessing the infrastructure of CPN was to determine what type of network technology would to

support the goals of the CPN. With only existing personnel available to design and implement the CPN, a division of labor and a phased approach was established. The planning approach maintained attainable goals, was streamlined, and could be completed in a five-year schedule. Throughout development and testing of the CPN, security of had to remain paramount. Degrading the security of MCEN during this phase would not be acceptable. Integrating the CPN into the existing security infrastructure was required. Hardware and software would have to be selected that would grow with the future demands placed on the CPN. Communication protocols for the CPN were evaluated for their capabilities against the needs of the CPN.

1. Network Technology

Asynchronous Transfer Mode (ATM) switching was chosen as a supporting technology for CPN. ATM was selected for its ability to meet the requirements of dynamic bandwidth management, traffic flow analysis, and ease of scalability. Visits were made to Department of Defense commands and industry sites that were using ATM in a manner similar to the plan the MITNOC envisioned. Administrators that were involved in a specific sites implementation of ATM were interviewed to capture lessons learned, and to determine the level of satisfaction with the performance of ATM technology. Following these site surveys, a series of vendors were evaluated to determine which was most likely to meet the current and future needs of the CPN.

2. Personnel Support

MITNOC engineers and planners could not increase personnel to handle the additional work created by establishing the CPN, a division of labor had to be created that made efficient use of personnel on hand. The approach used by the MITNOC staff was to divide the project into functional areas and corresponding phases. The phased approach will be discussed in detail in Section G, but for purposes of responsibility break down it is referred to here. During Phase I of implementation; the MITNOC network engineering and management section would plan and execute duties associated with the bottom three layers of the Open Systems Interconnect (OSI) model. Responsibilities in this phase primarily surround determining physical connections, equipment interfaces, and communication infrastructure. During Phases II and III, responsibilities shift to the MITNOC migration section, Headquarters Marine Corps (HQMC), and as the telecommunications community in the Marine Corps. HQMC and telecommunications personnel involvement will increase as the CPN becomes further established over time. During Phase I, all burdens are assumed by the MITNOC.

3. Security

Security of MCEN could not be compromised during the implementation of the CPN. It would be necessary to integrate CPN in a manner that would not degrade existing security of MCEN. Further, it makes sense to leverage the existing security infrastructure of MCEN. Figure 6 depicts the location of the firewall suite within the network

infrastructure. Entrance into the CPN from the Base Post or Station follows the firewall suite located at each location. The firewall suite screens inbound traffic from the CPN to the Base network before continuing to its final destination. By using existing hardware, security is maintained throughout the CPN.

4. Traffic Flow

The purpose of the screening router in Figure 6 is to screen and route all traffic according to packet content. Traffic flows from the protected region of the firewall suite to the screening router where it is filtered by destination. If the data packet reveals the destination to be a "usmc.mil" destination, it is routed to the CPN edge device and on to its "usmc.mil" destination. Traffic from outside the CPN, i.e. NIPRNET/Internet traffic never touches the CPN. Traffic from the NIPRNET/Internet is routed to the screening router, through the remainder of the security architecture, and on to its destination. This traffic flow management keeps traffic separated and secure.

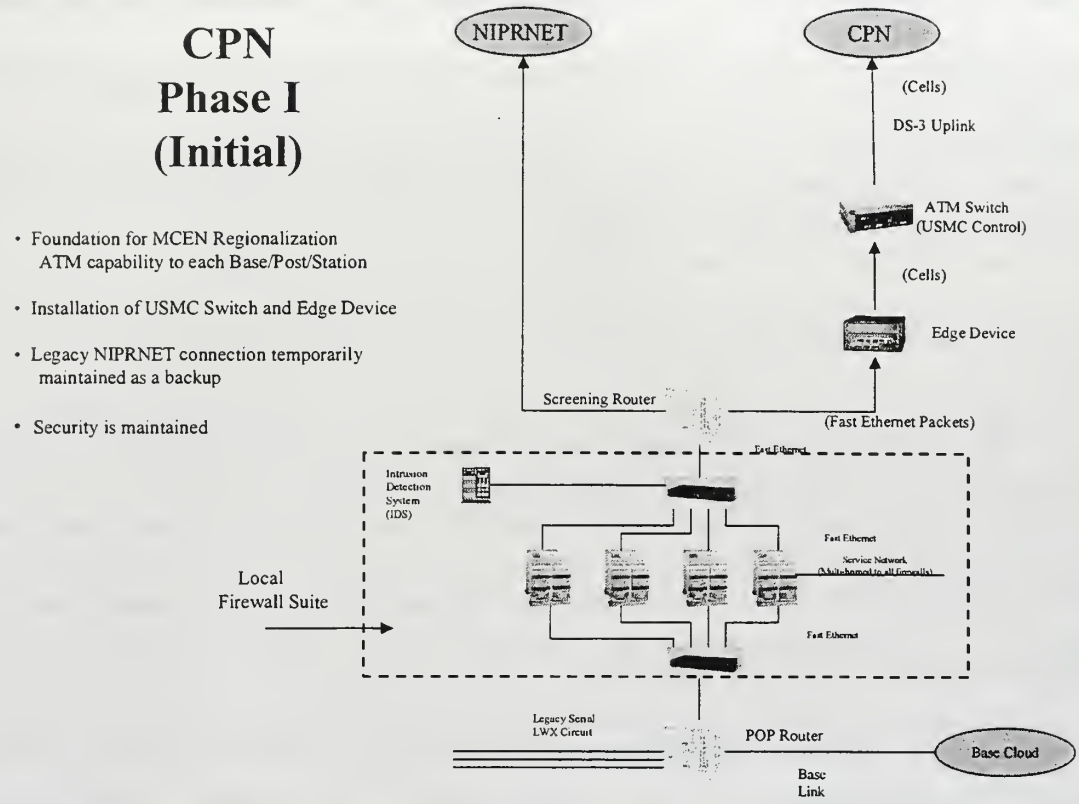

Figure 6. Collaborative Planning Network, Phase I.

5. Hardware

Additional hardware required to support the CPN is limited and consists of ATM switches, and Edge Devices. Each of these is explained below.

a. ATM Switch

The ATM switch lies at the perimeter of the CPN. Its purpose is to route and switch ATM cell traffic between other ATM switches in the CPN. ATM technology

is fast, reliable and easily scalable. The ATM switch also communicates with the Edge Device by sending ATM cells for conversion into Ethernet packets.

b. Edge Device

The Edge Device converts ATM cells to Ethernet packets and Ethernet packets to ATM cells. This enables communication between different protocols that are operating in each segment of the network.

6. Protocols

There are two main protocols required to operate the CPN on its different segments. For ease of management, it is desired to keep the number of protocols to a minimum to avoid confusion and complexity. All network equipment would require interoperability, while keeping protocols to a minimum. Between ATM switches, the protocol used is the Local Area Network Emulated (LANE) protocol. This protocol enables communication between ATM switches within the CPN. The Edge Device uses the Open Shortest Path First (OSPF) protocol. This protocol ensures that the shortest path is taken to the distant end. Protocol management, therefore, is streamlined and efficient with only two types being used.

G. CPN DESIGN AND ARCHITECTURE

The CPN consists of twenty-six locations that require ATM connection to build the network. These twenty-six locations were divided into seven Local Access Transport

Areas (LATAs) throughout the continental U.S., including Hawaii and Japan. Each location will connect to the ATM network via a DS-3 (45Mbps) communication link. Each access point consists of an ATM Switch, and an Edge Device that will provide the connection to the CPN. The screening router will connect to the Edge Devices for the CPN and DISN ATM switches to provide screening and segmentation of "usmc.mil" intranet traffic and all other non-intranet traffic. Figure 7 depicts the seven LATAs and Figure 8 shows the basic site topology.

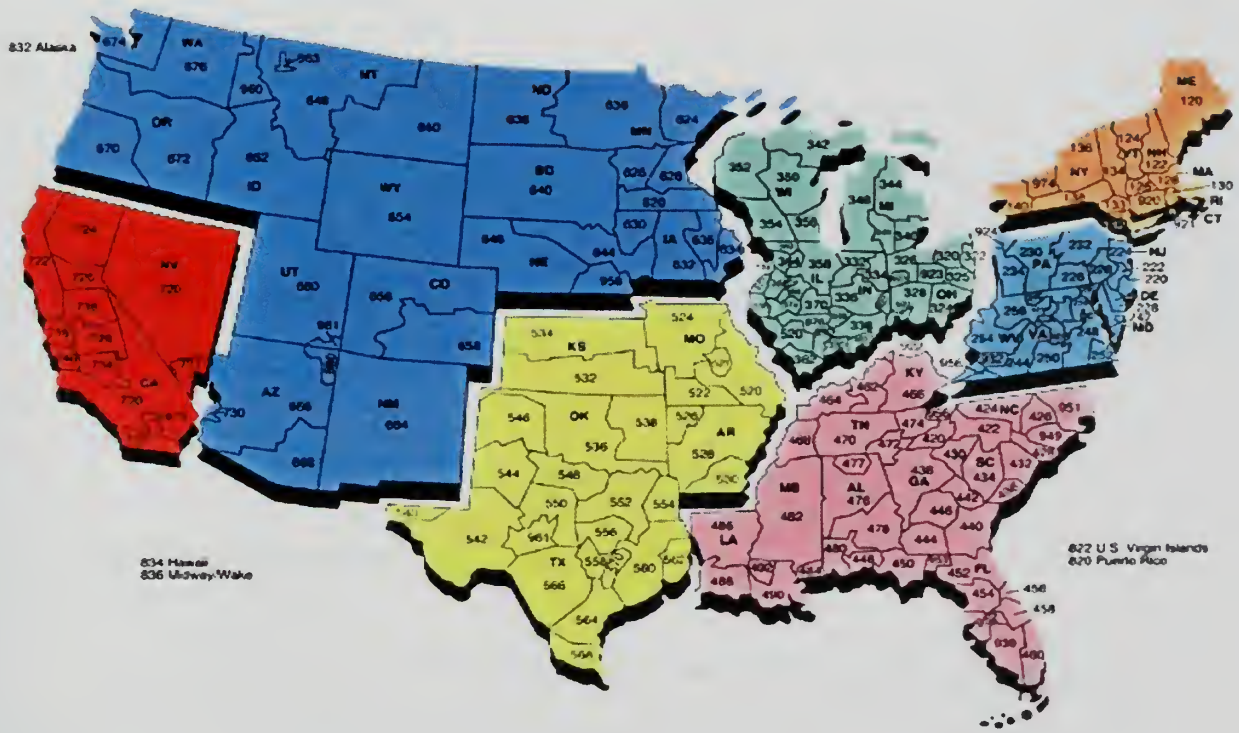

Figure 7. Local Access Transport Areas.

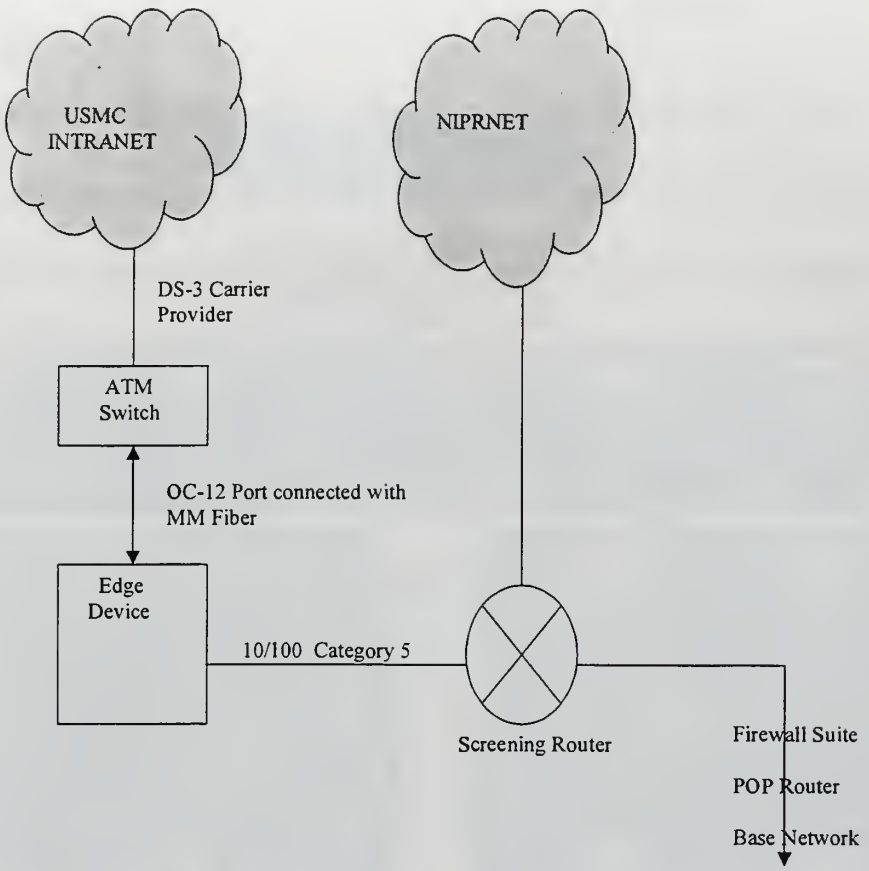

Figure 8. Basic Site Topology.

H. IMPLEMENTATION

Implementation of the CPN is planned as a three-phased approach anticipated to take approximately five years. This time phased approach is due to the complexity of the project and the physical distribution of sites that must be installed and configured. For the purposes of organization and network management, the CPN is subdivided into two Tiers. Each LATA represents Tier One, and locations that make up teach LATA, such as Bases, Posts, or Stations represent Tier 2.

1. Phase I

Phase I consists of establishing the basic communication infrastructure at each Tier One and Tier Two location. This includes installing ATM switches, Edge Devices and connecting to the ATM network and existing security infrastructure. During this phase, Tier Two locations remain connected to the NIPRNET as well as to the CPN to provide redundancy during migration. The completion of Phase I is achieved when all sites have successfully migrated to the new architecture and are accessing the NIPRNET and CPN simultaneously as required. Figure 9 depicts the physical topology at the completion of phase one.

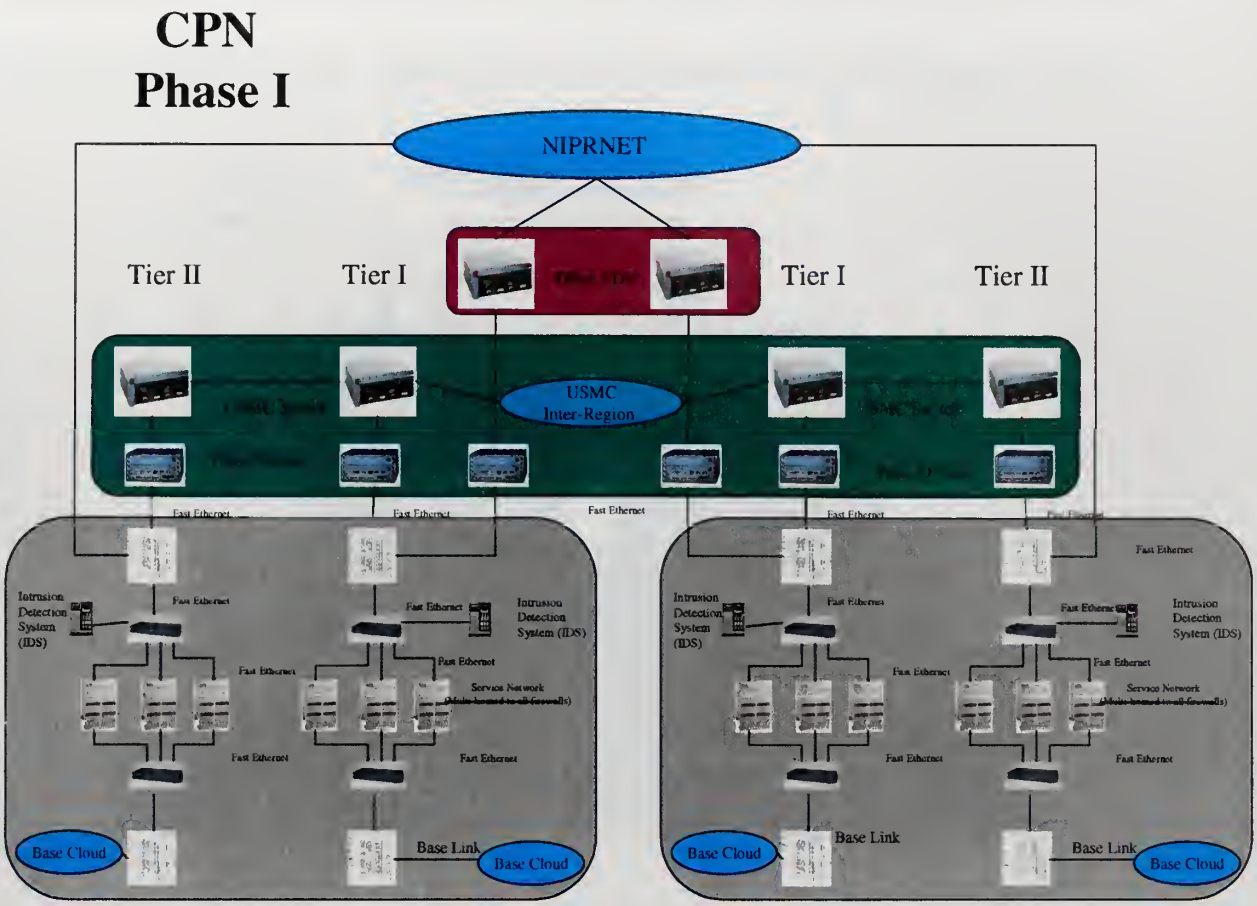

Figure 9. Phase I Completion.

2. Phase II

Phase II consists of collapsing the unclassified network and installing equipment necessary to support Phase III, the migration of SIPRNET to each LATA. Access to the SIPRNET is not currently available throughout the USMC. During this phase, Virtual Private Network (VPN) devices will be installed at each CPN access point. These devices

will tunnel secure paths via the CPN to support classified network traffic on the same circuit as unclassified traffic. Figure 10 depicts the network at the completion of Phase II.

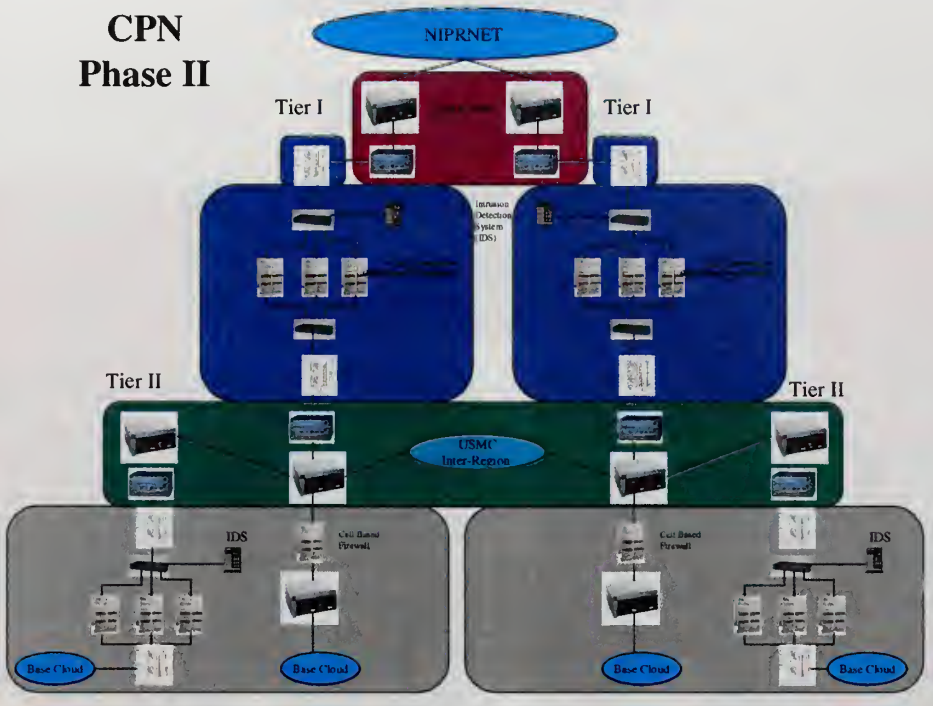

Figure 10. Phase II Completion.

3. Phase III

The successful migration of all internal "usmc.mil" traffic to the CPN will denote the completion of Phase III. SIPRNET access will be available at every Base, Post, and Station in the Marine Corps via VPN through the CPN. NIPRNET access is still active, providing access to the NIPRNET for all non-usmc.mil traffic. Figure 11 depicts the completion of Phase III.

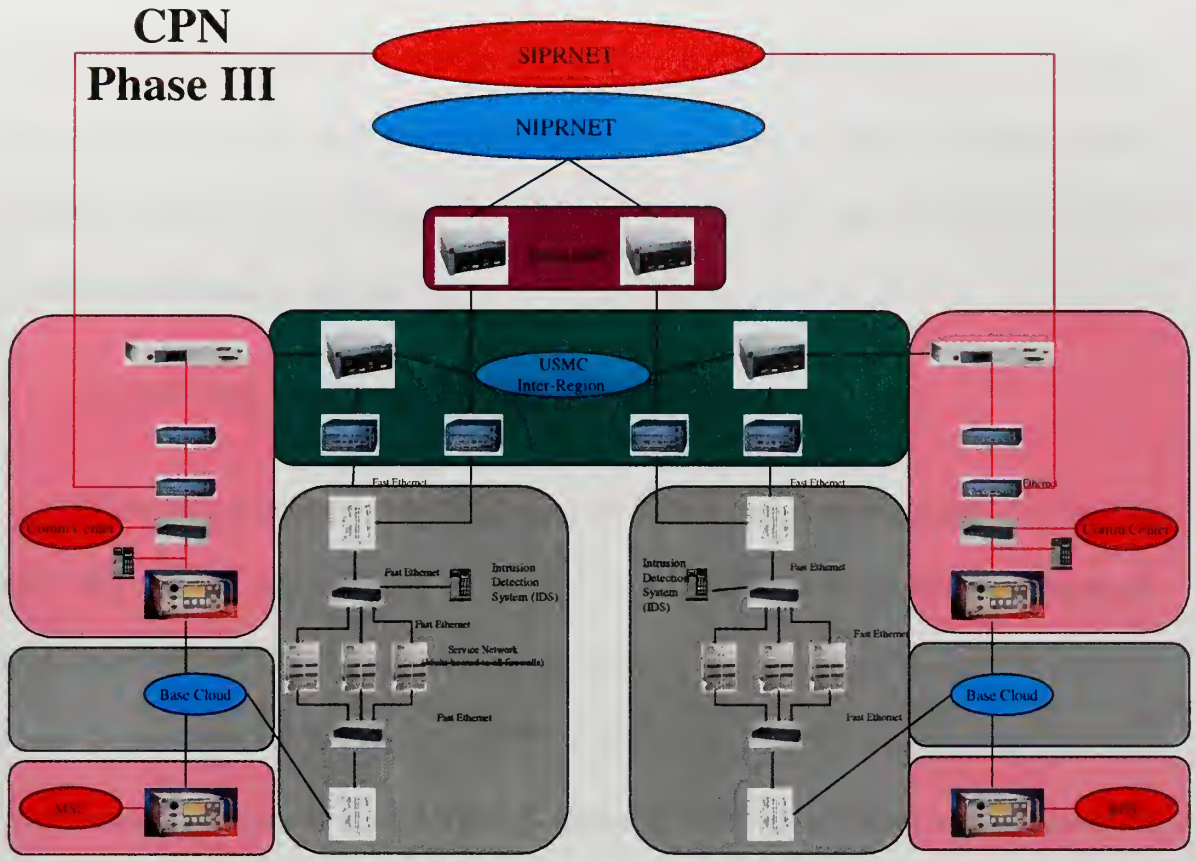

Figure 11. Phase III Completion.

I. METRICS

Current measurement tools used on the MCEN are rudimentary and do not provide detailed information necessary to evaluate and manage the network. As a result, new tools are being fielded by MARCORSYSCOM that will enhance network management and provide the ability to measure network load, execute traffic shaping, traffic analysis and dynamic bandwidth management. Currently, MITNOC uses an analysis tool that provides basic network information. Future network management tools

are being fielded at the time of this writing that are significantly more capable. These new tools will allow MITNOC personnel to effectively and efficiently manage the MCEN and CPN with real-time accuracy. Concorde Network Health and Net Scout will soon provide MITNOC managers and engineers with real time network information, making real time network configuration a reality.

J. EXPECTED BENEFITS OF IMPLEMENTATION

The primary reason for implementing the CPN is to increase quality of service to users. The current configuration of MCEN limits MITNOC's network management capabilities. The MITNOC does not have the ability to make dynamic bandwidth changes to best support users when required. The CPN will enable MITNOC network managers to better support their customers. MITNOC wants to improve detailed measurement of network performance. The CPN will enhance performance measurement capabilities of the MITNOC. An increased awareness of network performance trends and patterns will augment the ability of network administrators to anticipate and plan for varying needs of users on a global scale. Overall, quality of service and ease of use will move dramatically forward with the implementation of the CPN.

K. SUMMARY

With the current MCEN network infrastructure, quality of service and network management capability is limited. The MITNOC has developed a well thought-out plan to solve this problem and improve network performance on a USMC wide scale. By

creating an internal network controlled by Marines for Marines, MITNOC will be able to make real-time changes to support any network requirement. This global network will create a fulcrum that will improve network application research and development as well as routine tasks necessary to operate the Marine Corps in a network centric environment.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SUMMARY AND RECOMMENDATIONS

A. SUMMARY

Interest for intranets has continued to gain popularity over the last five years as many advocates proclaim successes from implementing this form of networking. Because of the advantages intranets offer, they will continue to replace existing disjointed internal networks. Benefits offered by intranets far outweigh other means of internal networking. With an intranet, organizations can distribute information from which people will pull what they need when they need it. Streamlined transaction processes can be implemented to control information input, reduce errors, and save money. Collaborative planning via an intranet can improve productivity and add to the bottom line.

Planning for and implementing intranets is a serious undertaking of systems engineering and should be approached in an organized manner beginning with a clear vision of the functionalities and benefits the project will deliver. IT projects can have significant impact on financial and staff resources and will impact an organizations project scheduling. For these reasons, planners must understand the impact an intranet project will have on an enterprise. By performing a detailed requirements analysis and assessment of existing infrastructure, organizations benefit from a thorough understanding of needs and capabilities required to support an intranet. Without thorough

assessment of requirements and the supporting infrastructure, an intranet project can quickly snowball into an expensive IT "fix-all" solution with minimal return.

B. RECOMMENDATIONS

There are many articles, publications, and books on the subject of intranet development. Many of these items deal at length with the technical aspect of planning and implementing an intranet. What is less common among intranet literature is information concerning how intranets have impacted the human side of organizations that claim success.

As the Department of Defense (DoD) and the Department of the Navy (DoN) begin to plan and implement intranets, some of grand scale; senior leaders and planners would do well to consider not only the technological changes that will take place, but also the human changes that will take place. Compared to technical issues to be solved, complex human changes required to make an intranet successful can be even more complex. [Ref. 7]

During intranet planning and development, senior leaders and decision makers should lean away from the technical aspects of planning and concentrate on the less-technical, not as clearly defined aspects of how the intranet will change and disrupt the very organization it is designed to help. Senior leaders and decision makers will find it natural to let technical problems work themselves out, while concentrating on how to leverage intranet technology to empower personnel rather than disrupt their routines.

C. SUGGESTED FURTHER STUDY

There are few cases in DoD and DoN where intranets have been successfully implemented. The USMC CPN is one of such cases. While this case is still in its infancy, it represents a clear thought process and methodology to planning, developing and implementing an intranet. What is not yet captured in the case study of this thesis is how the CPN will affect change and contribute to improved collaboration. Further analysis as CPN grows can contribute to success of other distributed computing projects by incorporating lessons learned during the CPN implementation.

As the Navy/Marine Corps Intranet (N/MCI) begins to get off the ground, studies of the first stages of implementation can provide lessons learned to benefit other sites further down the installation priority schedule. Many locations within the DoN can benefit from intranet technology. Further study on scaling intranet technology to improve distributed computing and collaboration will benefit DoN and the end users where intranets are introduced.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. INTRANET COST CALCULATOR SPREADSHEET

	Initial	Ongoing
Client Setup		
TCP/IP Stack		
Browser Software		
Machine Upgrades		
CPU		
Memory		
Hard Disk		
Operating System		
Other		
Total:	$0.00	$0.00
Server Setup		
Web server hardware		
Web server software		
Licensing Fee		
Installation		
Support		
Other server software		
Sever management		
News server		
Mail server		
Proxy server		
Search engine		
Database support		
Log analyzer		
Discussion software		
Chat software		
Other Costs		
Total :		
Content Creation		
HTML editors		
Graphics Editors		
Site management		
Java tools		
Javascript tools		
VBScripts tools		
ActiveX components		
Perl scripts		
Other CGI scripts		
Applications		
Other		
Total :		
Training Costs		
Intranet usage training		
Intranet publishing training		
Application development		
Server maintenance		
Help desk		
Other costs		
Total :		
Grand Total :		

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. INTRANET RELATED WEB SITES

1. http://www.100hot.com
2. http://www.metacrawler.com
3. http://hotbot.lycos.com
4. http://www.iorg.com/papers/
5. http://www.iorg.com/intranetorg/
6. http://www.process.com./intranets/wp2.htp
7. http://www.di.ufpe.br/~wise/textos-ingles/infraintra.html
8. http://www.amdahl.com/doc/products/bsg/intra/infra.html
9. http://www.amdahl.com/doc/products/bsg/intra/adapt.html
10. http://www.strom.com/pubwork/intranetp.html
11. http://ccf.arc.nasa.gov/~graves/amesweb/arcweb/index.htm
12. http://www.telecoms-mag.com/issues/199701/tcs/kennedy.html
13. http://www.ibm.com/services/e-business/infrastr.html

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Hoffer, J. A., J. F. George, and J. S. Valacich. 1998. *Modern Systems Analysis and Design.* 2nd ed. New York. Addison-Wesley.

2. Smith, Norman E. *Intranet Planning Guide, Parts 1-6.* 8 March 1999. Available [Online] http://www.intranetjournal.com/planning/030899_intraguide.html [27 March 2000].

3. Boyd, Charles. Management Issues. NO DATE. Available [Online] http://www.mgt.smsu.edu/mgt487/mgtissue/newstrat/moore.htm [19 July 2000].

4. Telleen, Stephen D. *Intranet Organization, Chapter 8, Planning and Implementation* March 1997. Available [Online] http://www.iorg.com/intranetorg/chpt8.html [27 March 2000].

5. Hegering Heinz-Gerd, and Lapple, A. 1993. *Ethernet, Building a Communications Infrastructure.* New York. Addison-Wesley.

6. Comer, Douglas E., 1999. *Computer Networks and Internets.* 2nd ed. Upper Saddle River, New Jersey. Prentice-Hall.

7. Brenton, Chris. 1999. *Mastering Network Security.* San Francisco, Sybex.

8. Pfleeger, Charles P. 1997. *Security in Computing.* 2nd ed. Upper Saddle River, New Jersey. Prentice-Hall.

9. Koehler, Jerry W. et al. 1998. *The Human Side of Intranets, Content, Style, and Politics.* New York, St. Lucie Press.

10. Hills, Melanie. 1997. *Intranet Business Strategies.* New York. Wiley Computer Publishing.

11. Guengerich, Steve et al. 1997. *Building the Corporate Intranet.* New York. Wiley Computer Publishing.

12. Gonzales, Jennifer S., 1997. *The 21st Century Intranet.* Upper Saddle River, New Jersey. Prentice-Hall.

13. Greer, Tyson. 1998. *Understanding Intranets*. Redmond, Washington. Microsoft Press.

14. Rich, Oliver E. and Valerie S. Rich, *Intranet Technology: Considerations for Implementation Within the Department of Defense*, Master's Thesis, Naval Postgraduate School Monterey, California, March 1997.

15. Matheson, Paul G., March 1999. *An Operational Intranet for Fighter Composite Squadron Thirteen (VFC-13)*, Master's Thesis, Naval Postgraduate School, Monterey, California.

16. Rutherford, Emelie, April 2000. *Is This Any Way to Build an Intranet? CIO Magazine Available* [Online] http://www2.cio/archive/040100_intranet_content.html [April 2000].

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Director, Training and Education 1
   MCCDC, Code C46
   1019 Elliot Road
   Quantico, VA 22134-5027

4. Director, Marine Corps Research Center 2
   MCCDC, Code C40RC
   2040 Broadway Street
   Quantico, VA 22134-5107

5. Marine Corps Representative 1
   Naval Postgraduate School
   Code 037, Bldg 330, Ingersoll Hall, Room 116
   555 Dyer Road
   Monterey, CA 93943

6. Marine Corps Tactical Systems Support Activity 1
   Technical Advisory Branc
   Attn: Librarian
   Box 555171
   Camp Pendelton, CA 92055-5080

7. Professor Barry A. Frew, Code SM/Fw 1
   Naval Postgraduate School
   Monterey, CA 93943

8. Professor William J. Haga, Code SM/Hg 1
   Naval Postgraduate School
   Monterey, CA 93943

9. Space and Naval Warfare Systems Command.....1
4301 Pacific Highway Bld. OT2 Rm. 217
San Diego CA 92110-3127

10. Chief of Naval Operations (N6).....1
2000 Navy Pentagon
Washington D.C. 20350-2000

11. Professor Barry A. Frew, Code 01E/Fw.....1
Naval Postgraduate School
Monterey, CA 93943

12. Professor William J. Haga, Code SM/Hg.....1
Naval Postgraduate School
Monterey, CA 93943

13. Mr. Steven H. Page.....1
Head, Network Engineering Branch
United States Marine Corps Information Technology Network Operation Center (MITNOC)
Quantico, VA 22134

14. Major Scott R. Sizemore.....1
9803 Woodfall Court
Burke, VA 22015

15. Chair, Information Systems Academic Group.....1
Code IS
Naval Postgraduate School
Monterey, CA 93943